B2 Cont.

example a computer, with which the electronic postage stamp is printed is thereto provided with a Postal Security Device (PSD), to which a unique identification code is related. The electronic postage stamp comprises various elements, of which a few are mentioned as "security critical": the identification code of the PSD, the value of the contents of an incremental register, the franking value of the postal article and a digital signature. The contents of the incremental register represent the total monetary value of all hitherto printed electronic postage stamps with the related PSD. The combination of identification code and the contents of the incremental register represents a unique bit string per postal article. Since the manner in which said unique bit string is composed must comply with a known rule, the value of a following unique bit string for a following electronic postage stamp can be predicted, which is disadvantageous in regard to possible fraud.--

Page 3, between lines 11 and 12, insert the following heading:

--SUMMARY OF THE INVENTION--.

Page 3, replace the fourth full paragraph as follows:

B3

--According to the invention, each unique bit string used is thus centrally generated and registered, and said bit string is moreover coupled to the user who has bought an electronic postage stamp and/or the machine which prints the electronic postage stamps. It can thus not only be centrally detected whether the electronic postage stamps are used only once, but fraud can also be easily traced to the source. Further, the use of a PSD can thereby possibly be waived.--

Page 3, replace the last paragraph bridging pages 3 and 4, as follows:

B4

--In a first embodiment, the unique bit string and the identification code, protected with the aid of a first message authentication code and/or protected by encoding, are stored, prior to step c, by a terminal on an information carrier with memory, step c taking place after the information carrier has been read in by a printing device. Such an information carrier can, for example, be a chip card, on which several such unique bit strings, together with the identification code, can be stored. The identification code can, for example, be derived from the number of the bank or ATM (Automated Teller Machine) card with the aid of his personal identification number (PIN).--

Page 6, delete lines 34 and 35.

Page 7, replace the first full paragraph as follows:

B5

--The present invention is also related to an exchange provided with a first central memory having a set of unique bit strings, a second central memory for storing the combinations of identification codes and provided unique bit strings, said combinations corresponding with franking marks which have been printed on a document, central input means for inputting franking marks printed on documents, a third central memory for storing combinations of identification codes and unique bit strings present on the inputted franking marks, and processor means connected to the central input means and the first, second, third central memories for mutually comparing the data in the second and third central memories. An "exchange" as used in the present application refers to a central station that has the first, second and third central memories.—

Page 8, between lines 20 and 21, insert the following heading:

--BRIEF DESCRIPTION OF THE DRAWINGS--.

Page 9, between lines 7 and 8, insert the following heading:

--DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS--.

Page 9, replace the paragraph beginning at line 8, as follows:

B6

--In Fig. 1, reference number 2 refers to a terminal, which, for example, is set up in the wall of a post office. Said terminal 2 can communicate with a central station or an exchange 34, for example via the public switched telephone network (PSTN) 46. Communication paths via other networks are of course possible. In this case, use can be made of the Internet. Communication can also take place in other ways, for example via CDROMs, floppy disks, etc.–

Page 11, replace the fifth paragraph as follows:

B7

--Said information 29 comprises, for example, human-readable data 24 related to the mail-sending organization (or other advertising), as well as a marking sign 26 (for example a bar code) enabling automatic orientation of the postal article in a stamping/sorting machine, and a franking mark 28, for example in the form of a two-dimensional bar code 28, which contains further, possibly encoded, information. Said franking mark 28 shall at least contain a unique bit string,

B7 Cont.

of which the use will be explained further on, and an identification code. The identification code identifies the user, i.e. the person who purchased the electronic postage stamp, and/or the device with which the franking mark is printed. If the identification code is coupled to the printing device, this can, for example, be a unique code associated with said SAM 19. In that case, the owner of the franking machine is responsible for possible fraud with the use of electronic postage stamps.--

Page 15, replace the second full paragraph as follows:

B8

--For further protection of the whole, the processor 4 preferably sends a copy of the identification code with the issued franking numbers, protected by MAC1 and/or protected by encoding, to the exchange 34, which stores this information in memory 40 so that at a later stage possible fraud can be checked centrally, step 218. This will be further discussed later.--

Page 17, replace the third full paragraph as follows:

B9

--Upon dispatch of the postal article 22 from a sender to a receiver, said postal article 22 will, at a given time, arrive in a sorting center. There said postal article

B9 Cont.

22 will be read in with the aid of the means 32, and it can be checked again whether said postal article 22 has been sufficiently franked. The means 32 read at least the franking mark 28. The means 32 thus collect all read-in franking marks 28 of all postal articles which are provided therewith. All franking marks 28 are subsequently sent to the exchange 34 and are there read in by the processor 36 via the input means 44. Said processor 36 stores the inputted franking marks in the memory 42.–

Page 22, replace the last paragraph bridging pages 22 and 23, as follows:

B10

--A further option is to implement the system shown in Fig. 1 in such a manner that each of the franking cards 18 is also allocated a unique number. Possible fraud with franking cards 18 can then be pin-pointed. Information related to said fraudulently used franking cards 18 can then be included on an arbitrary franking card 18. Subsequently, said information, related to the fraudulently used franking cards 18, can then be transferred “unperceived” to the franking machines 20, which store the related information in a memory (not shown). If a customer with fraudulently used franking card 18 wishes to print an electronic postage stamp, the franking machine 20 can detect the related franking card 18 and render it invalid. This can be done either by deleting

B10 cont.

the contents of the franking card 18 or making them non-readable, or by simply refusing to print an electronic postage stamp. Thereby further damages by possible fraud can be decreased.-

Page 24, replace the third full paragraph as follows:

B11

--Fig. 4a shows a flowchart of an embodiment of the functioning of the PC 50 in the context of the present invention for reloading a bank card 18 with a certain desired amount to be spent on electronic stamps. Fig. 4b relates to the actual printing of such an electronic stamp with such a bank card 18.--

Page 27, replace the last paragraph bridging pages 27 and 28, as follows:

B12

--It is also imaginable, however, to let payment be made later, as explained above with reference to the embodiment of Fig. 1. In that regard, the balance loaded in the bank card 18 does not represent a total amount which can be expended on electronic stamps, but the number of times that the franking number provided can be used. The advantage of post-payment is that the user does not need to weigh his postal article 22 in advance in order to have the correct franking value included in the franking mark 28. After all, the franking mark here too uniquely identifies the user, who can subsequently have the invoice sent to him or whose bank balance can be automatically debited. Moreover, the presence of the unique franking number with identification code and the actual "balance" guarantees that each postal article 22 is uniquely identified, so that fraud can be detected immediately.–

Page 28, replace the first full paragraph as follows:

B12

--It is further remarked that, instead of or together with an identification of the user, it is possible to include an identification of the SAM 64 in the franking mark. In that case, the owner of the PC 50 with SAM 64 is responsible for the correct payment of the electronic postage stamps and for possible fraud carried out with the PC 50. It is then up to said owner to subject access to the program for purchasing an electronic postage stamp to authorization rules.--

Page 28, replace the second full paragraph as follows:

--In a further embodiment with the aid of a PC 50, a standard PC without SAM 64 can be used. In this case, said PC 50 cannot safely calculate MAC's. The franking mark is then